

---

# *Components of a Biosecurity Program*

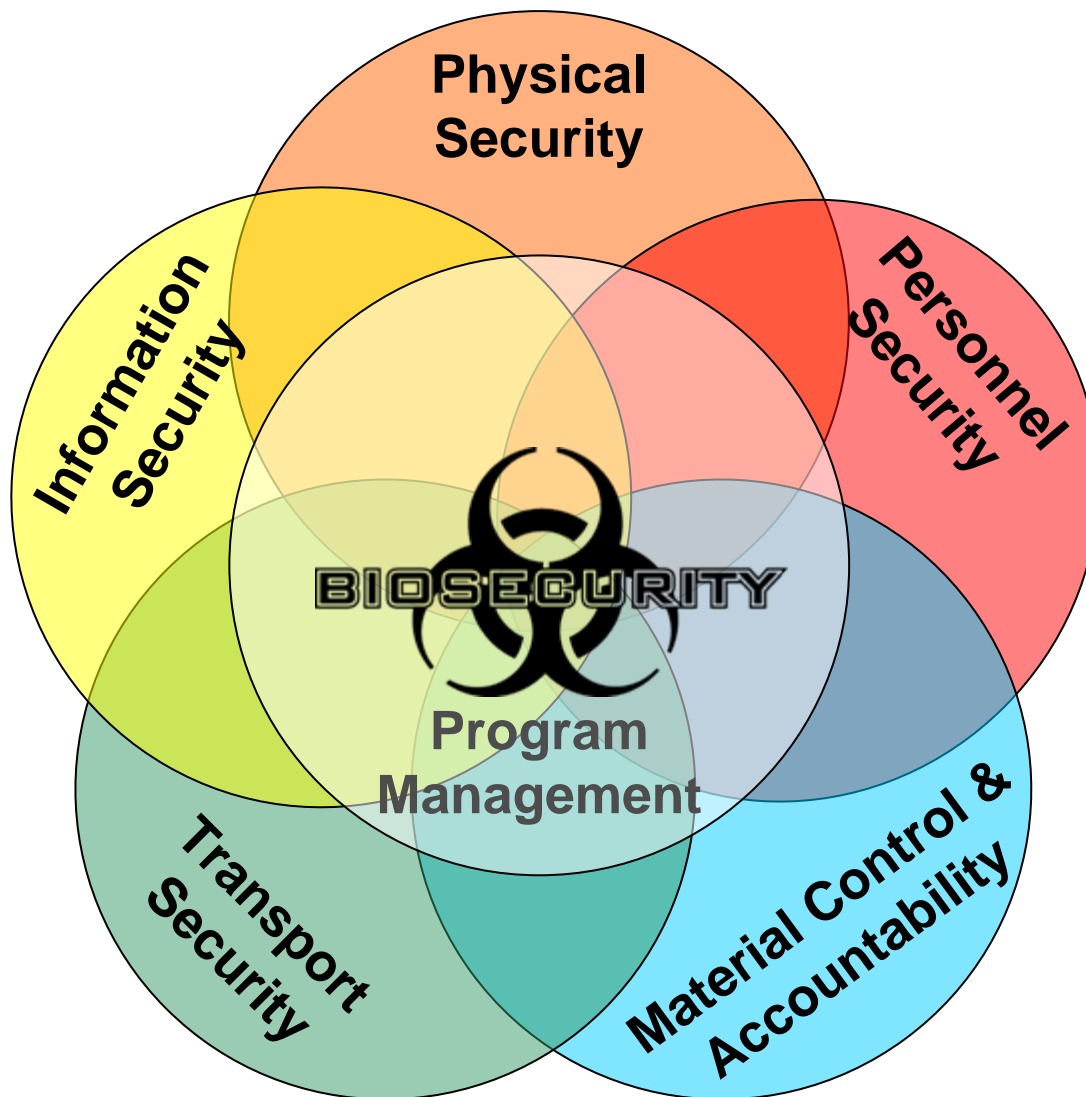
**SNL Biosecurity Team**  
**Chemical & Biological Weapons Nonproliferation**  
**International Security Center**  
**October 23, 2005**

SAND No. 2005-3290 C

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,  
for the United States Department of Energy's National Nuclear Security Administration  
under contract DE-AC04-94AL85000.

# Components of Biosecurity

---



# Physical Security: System Elements

---

- Graded protection
- Access control
- Intrusion detection
- Alarm assessment and response



# Physical Security:

## Concentric Layers of Security

---

- **Property Protection Areas**

- **Low risk assets**

- Grounds
    - Public access offices
    - Warehouses

- **Limited Areas**

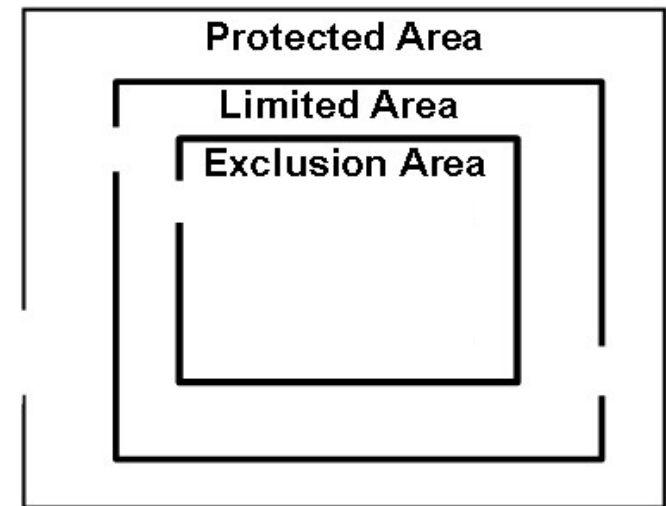
- **Moderate risk assets**

- Laboratories
    - Sensitive or administration offices
    - Hallways surrounding Exclusion Areas

- **Exclusion Areas**

- **High risk assets**

- High containment laboratories
    - Computer network hubs



# Physical Security: Property Protection Control

---

- **Fences**
  - **Mark the boundaries of your property**
  - **Announce your intention to protect the property**
  - **Elicit strong statement of intent from intruder**
  - **Terrain features can also serve this purpose**

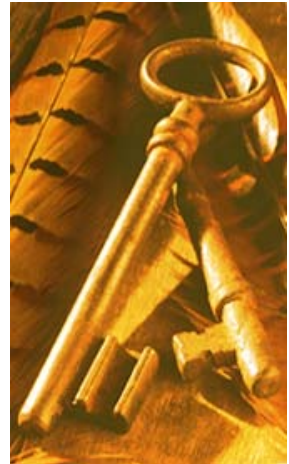


# Physical Security:

## Limited and Exclusion Area Access Control

---

- Access control ensures that only authorized individuals are allowed into certain areas
  - Increasingly strict controls as you move toward highest risk assets
- Limited Areas
  - Requires unique credential for access
    - Electronic key card, or
    - Controlled key
- Exclusion Areas
  - Requires unique credential and unique knowledge for access
    - Electronic key card and keypad or biometric device, or
    - Controlled key and second individual to verify identity



# Physical Security:

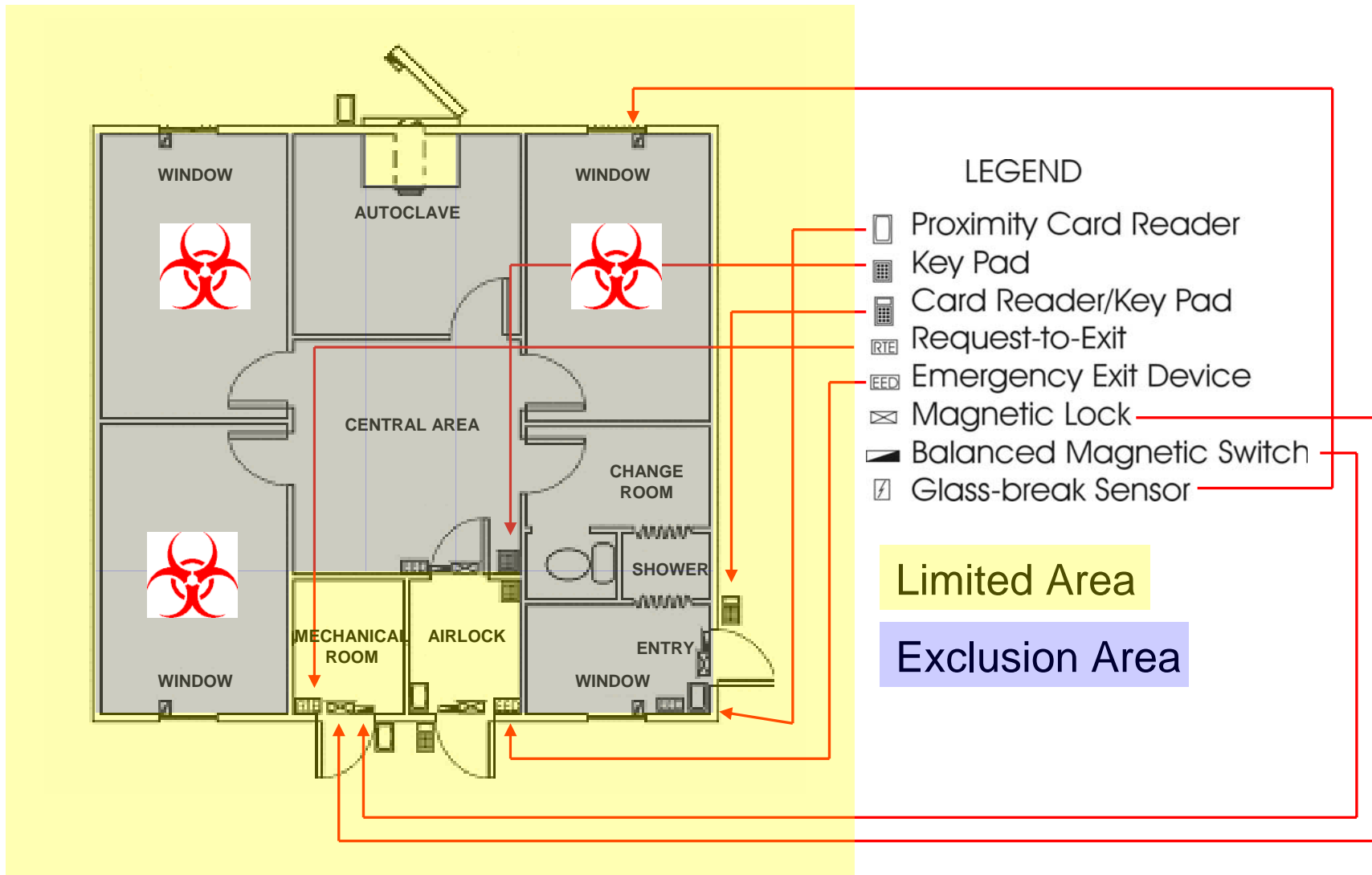
## Intrusion Detection and Response

---

- **Security violation detection**
  - Guards
  - Electronic sensors
- **Alarm assessment**
  - Validation of violation before response
  - Can be direct (guards) or remote (video)
- **On-site guard force response**
  - Supports electronic systems
  - Patrols or guards perimeter and buildings
  - Summons and directs local law enforcement
- **Local law enforcement (police) support**
  - Reinforces or substitutes for on-site guard force
  - Memorandum of understanding

# Physical Security:

## Example Laboratory Building





# Physical Security: Procedures

---

- **Examples of procedures that can be implemented to achieve graded protection**
  - **Impose consequences for security violations**
  - **Log personnel (including visitor) access to restricted areas including entry and exit times**
  - **Establish controls on animal and supply handling**
  - **Enforce escort policies**
    - **Visitors**
    - **Maintenance and cleaning personnel**
    - **Delivery personnel**
  - **Train personnel on what to do about:**
    - **Unrecognized persons**
    - **Unusual or suspicious activity**

# Physical Security:

## Performance Testing and Maintenance

---

- **Create security performance test plan and procedures**
- **Schedule periodic testing of hardware and policy implementation**
- **Schedule periodic testing of response force procedures**
- **Document test results**
- **Take corrective action**
  - **Schedule maintenance and repair of hardware**
  - **Corrective training and policy adjustments as appropriate for policy implementation failures**
  - **Corrective training and exercises for guard force**

# Personnel Security

---

- **Personnel Screening**
- **Badges**
- **Visitor Control**
- **Training**



# Personnel Security: Screening

---

- **Conduct screening for authorized individuals**
  - Degree of scrutiny commensurate with level of risk associated with the position
    - Need for unescorted access to restricted areas
    - Types of assets held in the restricted areas
    - Level of authority in association with high risk materials
- **Mechanisms**
  - Verify credentials
  - Check references
  - Criminal history
  - In-depth background investigation



# Personnel Security:

## Visitor Controls

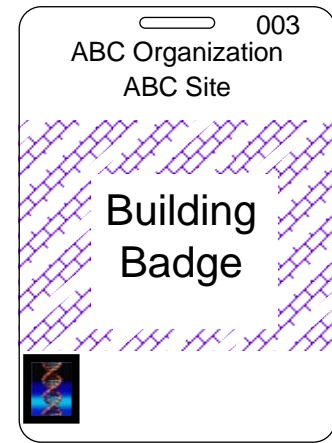
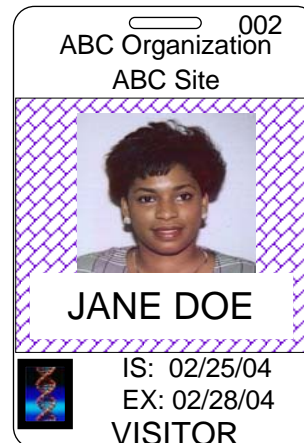
---

- **Types**
  - **Personal Visitors**
    - Family members
  - **Casual Visitors**
    - Tours, seminars
    - Equipment repair technicians
  - **Working Visitors**
    - Visiting researchers
    - Facility maintenance personnel
- **Controls**
  - All visitors should have a host at the facility
  - Visitors should be escorted in restricted areas

# Personnel Security:

## Badges

- **Badges should be issued to those individuals authorized to be in restricted areas**



- **Badge return**
  - Upon employee termination
  - Daily or at the conclusion of a limited term for visitors
- **Report lost or stolen badges**

# Personnel Security:

## In-Processing and Out-Processing

---

- **In-Processing**
  - Complete all required forms, safety training, security training and immunizations as applicable for work environment
  
- **Out-Processing**
  - Access changes or termination
  - Retrieve property
  - Deactivate computer and electronic access accounts



# **Personnel Security:**

## **Employee Assistance Program**

---

- **Provide resources to address problems associated with a variety of personal issues**
  - **Marital issues**
  - **Family issues**
  - **Eldercare/childcare issues**
  - **Job conflict**
  - **Grief**
  - **Financial issues**
  - **Legal issues**
  - **Stress**



# Personnel Security: Security Violations

---

- **Security violations should be ranked according to the effects upon the organization**

Organization ABC keeps  
large quantities of  
HMUR agents in  
Building 1, Room 123,  
Freezer A.



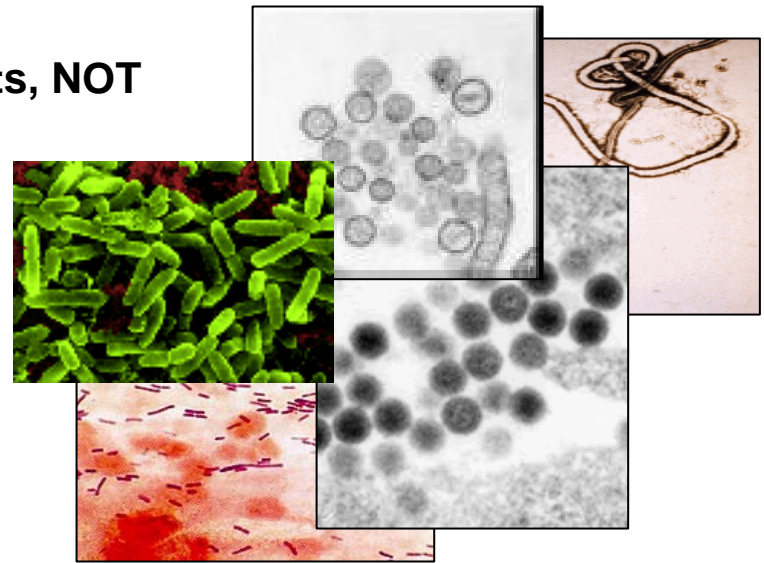
# Material Control & Accountability: Objective

---

- **Ensure the complete and timely knowledge of:**
  - What materials exist
  - Where the materials are
  - Who is accountable for them
  
- **NOT: to detect whether something is missing**

# Material Control and Accountability

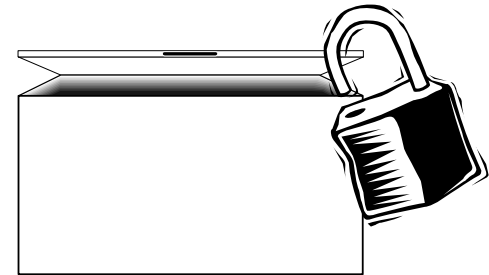
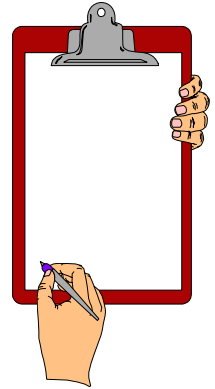
- Defining “material” is complicated
- Agent
  - Name and description
- Quantity
  - Based on containers or other units, NOT number of microbes



# Material Control and Accountability

---

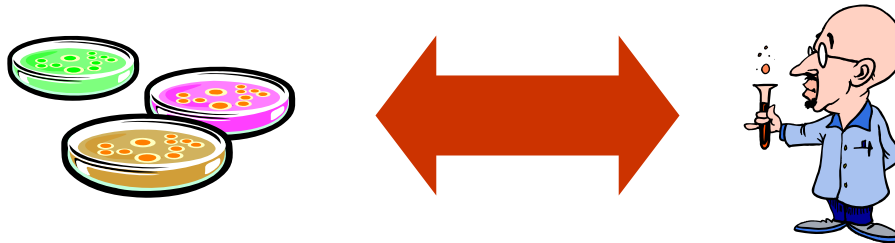
- Control is either...
  - Engineered / Physical
  - Administrative
- Containment is part of material control
  - Containment Lab / Freezer / Ampoule
- Procedures are essential for material control
  - For both normal and abnormal conditions



# Material Control and Accountability

---

- All material should have an associated “accountable person”



- Procedures should ensure accountability

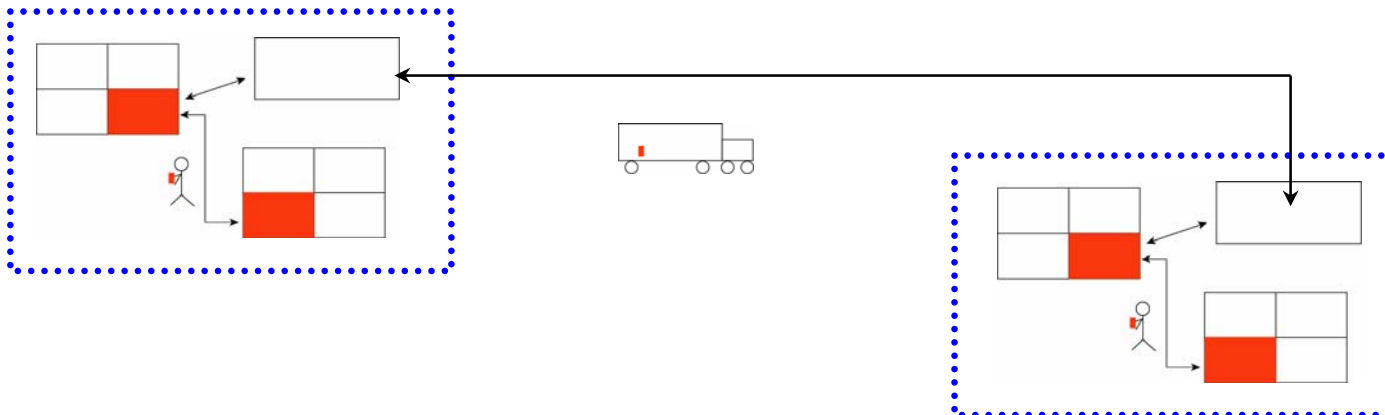
# Material Control & Accountability: Challenges and Benefits

---

- **We want to *avoid*...**
  - Implementing poor MC&A measures
  - Making “real work” more burdensome
  - Imposing unacceptable costs: time / money / effort
  - Spreading knowledge of inventory information
  
- **Benefits**
  - Prevents, or makes more difficult, some easy material diversion scenarios
  - Documents lab status *before* any problems occur
    - Better than forensic work *afterwards*
  - Is consistent with and reinforces good laboratory practice

# Material Transport Security

- **Why?**
  - Dangerous pathogens and toxins are vulnerable to theft during movement outside of protected areas
- **Who?**
  - Facilities, carriers, and states all responsible
- **The goal of transport security is**
  - To mitigate the risk of theft during transport



# Transport Security: Chain of Custody

---

- **Aims to protect sample by documenting**
  - All individuals who have control of sample
  - Secure receipt of material at appropriate location
- **Chain of custody documentation includes**
  - Description of material being moved
  - Contact information for a responsible person
  - Time/date signatures of every person who assumes control





# Transport Security: Facility Responsibilities

---

- **Personnel management**
  - For people who have access to dangerous pathogens and toxins or information during transfers
- **Establish chain of custody (CoC)**
  - Record all individuals who have contact with the dangerous pathogens and toxins
- **Provide physical security**
  - For packages that need temporary storage
- **Protect transport documentation**
- **Determine who is able to authorize, transport, and receive dangerous pathogens and toxins**

# Transport Security: Process

---

- **Responsible authority pre-approves all transport**
- **Transport should be documented in lab records**
- **Transport is controlled and documented in delivery records**
- **Timely shipping methods are used**
- **Chain of Custody is maintained**
- **Notification of successful receipt**

# Information Security

---

- **Protect information that is too sensitive for public distribution**
  - Label information as restricted
  - Limit distribution
  - Restrict methods of communication
  - Implement network and desktop security
  
- **Biosecurity-related sensitive information**
  - Security of dangerous pathogens and toxins
    - Risk assessments
    - Security system design
  - Access authorizations



# Information Security:

## Identification, Control, and Marking

- **Identification**

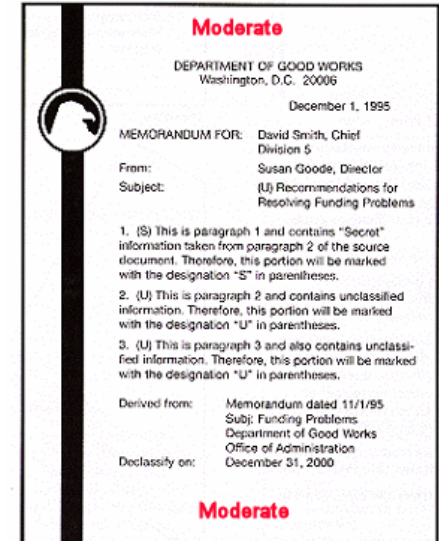
- Users of information should know the information's designated sensitivity level
- Levels of sensitivities should be based on standards
  - Low, Moderate, High
- A review and approval process aids in the identification of sensitivities
  - Critical for public release of information

- **Control**

- The control of moderately and highly sensitive information should be the direct responsibility of the individual with the information
- This includes the physical security of the information and places where the information is stored
- In order to refuse public access upon request, information must be exempt from FOIA

- **Marking**

- Moderately and highly sensitive information should be labeled in a consistent manner
  - Sensitivity level designation
  - Top and bottom of each page / cover sheet
- Marking and control methods should be well understood by those working with information



**Moderate**

DEPARTMENT OF GOOD WORKS  
Washington, D.C. 20006

December 1, 1995

MEMORANDUM FOR: David Smith, Chief  
Division 5

From: Susan Goode, Director

Subject: (U) Recommendations for  
Resolving Funding Problems

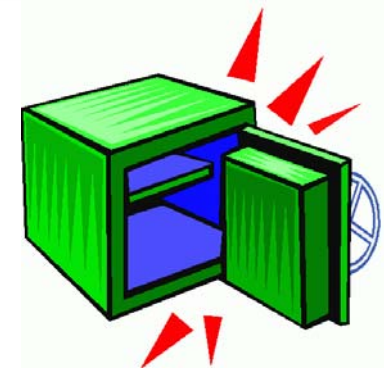
1. (S) This is paragraph 1 and contains "Secret" information taken from paragraph 2 of the source document. Therefore, this portion will be marked with the designation "S" in parentheses.

2. (U) This is paragraph 2 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

3. (U) This is paragraph 3 and also contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

Derived from: Memorandum dated 11/1/95  
Subj: Funding Problems  
Department of Good Works  
Office of Administration  
Declassify on: December 31, 2000

**Moderate**



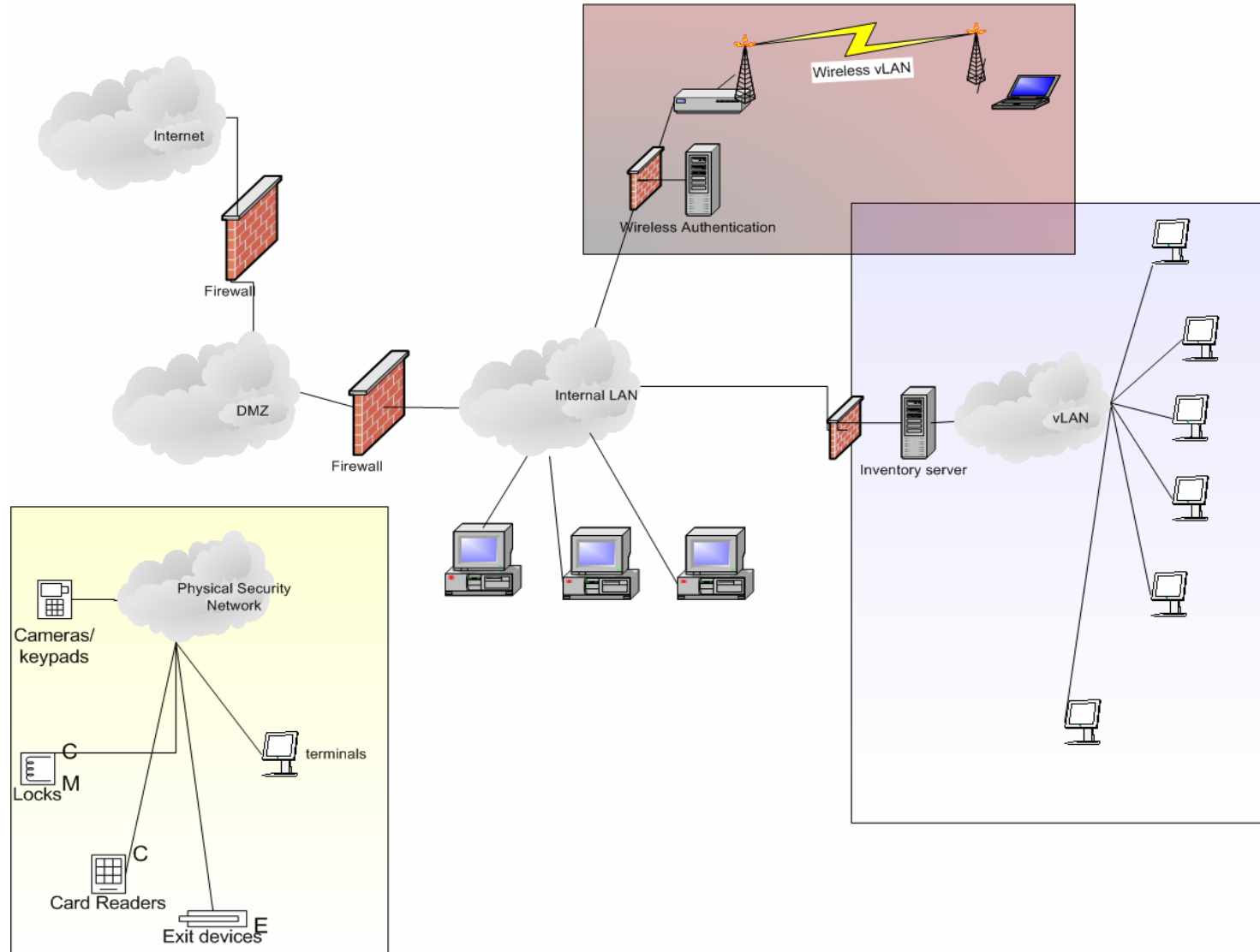
# Information Security:

## Communication and Network Security

---

- **Insecure transmission of information can lead to accidental release**
  - Mail, email, or fax security is required
  - Limited discussions in open areas
  - Information should only be reproduced when needed and each copy must be controlled as the original
- **Network Management**
  - The network on which all information is transmitted and systems on the network should be protected
    - Infrastructure
    - Servers
    - Network layered access
    - Desktop security
    - Remote access
    - Wireless

# Example Network Design



# Program Management: Responsibilities

---

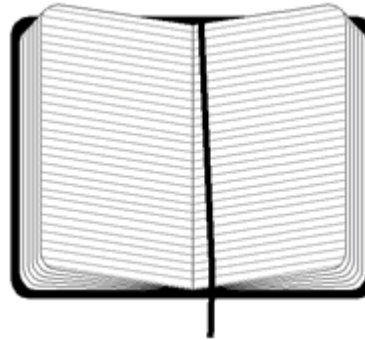
- **Identify the protection objectives of the biosecurity system**
  - Distinguish between “unacceptable” and “acceptable” risks
  - Ensure that the cost to protect an agent is proportional to the risk of malicious use
- **Design the system**
  - Physical security
  - Security policies and procedures
- **Write security and emergency response plans**
- **Conduct regular training and internal reviews**
- **Allocate resources**



# Program Management: Biosecurity Training

---

- Annual training tailored to different audiences
  - New and current employees
  - Managers
  - Emergency responders



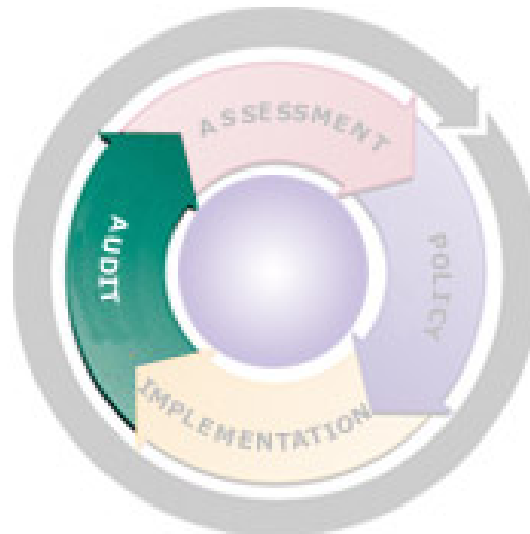


# Program Management:

## Self Assessments and Management Reviews

---

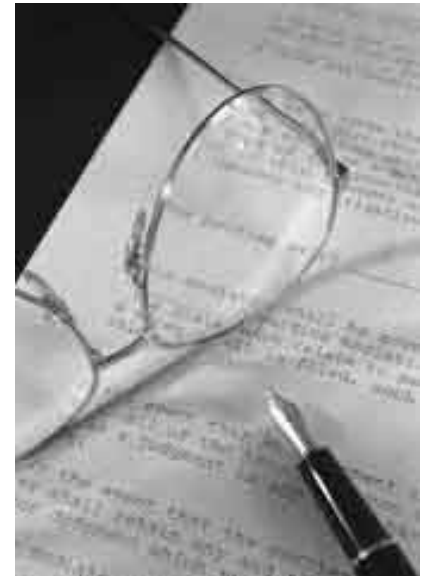
- **Self assessments ensure compliance with standards and evaluate effectiveness of the biosecurity program**
- **Management reviews institute corrective and preventive actions, and allocate required resources**



# Program Management: Laboratory Biosecurity Plan

---

- **Develop laboratory biosecurity plan**
  - Facility mission and description
  - Risk definition(s)
  - Physical security
  - Personnel management
  - Material control and accountability
  - Material transfer security
  - Information security
  - Biosecurity program management
  - Incident response plans and reporting



# Program Management: Policies

---



- **Realistic policies**
  - Policies should be comprehensive
  - Policies should allow for users to work as needed
  
- **Understanding of policies by all users**
  - Having clear policies is critical to users following them
  - The policies should be easy to locate, understand, and follow

# Result of Biosecurity Risk Management

---

- **Most pathogens and toxins would likely be LMUR**
- **Most current Select Agents would likely be MMUR**
- **Security associated with LMUR and MMUR would be achievable at reasonable cost for the broad biological research community**
  - **Rely largely on existing biosafety measures**
- **Very few Select Agents would be HMUR or EMUR**
- **Security for facilities that work with HMUR or EMUR would be relatively significant, but should still**
  - **Rely largely on policies and procedures**
  - **Be transparent to the users**
  - **Use resources efficiently**
  - **Not unnecessarily hinder normal operations (e.g. research, diagnostics, biosafety)**

# Conclusions

---

- **Necessary to take steps to reduce the likelihood that the *high risk agents, or any agents stipulated by government regulation*, could be stolen from bioscience facilities**
- **Critical that these steps are designed specifically for biological materials and research so that the resulting system will balance science and security concerns**
- **Biological facility risk mitigation may be accomplished through an integrated biosecurity system that incorporates policies, procedures and equipment**